

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-321749

(43)Date of publication of application : 12.12.1997

(51)Int.Cl. H04L 9/14
G06F 15/00
G09C 1/00
H04L 9/10

(21)Application number : 08-134823

(71)Applicant : CHUBU NIPPON DENKI
SOFTWARE KK

(22)Date of filing : 29.05.1996

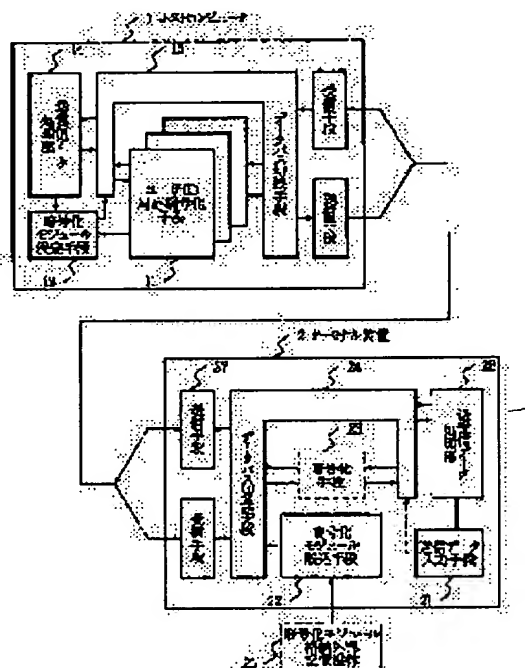
(72)Inventor : NANJO MASAYUKI

(54) ON-LINE SECURITY CONTROL SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an on-line security control system capable of improving security at an on-line system by enciphering data to transmit/receive between a host computer and a terminal device after log on.

SOLUTION: After checking the propriety of use ID, the host computer 1 selects a user ID corresponding enciphering means 11 corresponding to the user ID to encipher and decode characteristically to the user. In addition, the terminal device 2 reads an enciphering module characteristic to the user to an enciphering means 23 from a portable external storage medium body 25 to encipher and decode characteristically to the user to secure security.



LEGAL STATUS

[Date of request for examination] 29.05.1996

[Date of sending the examiner's decision of rejection] 16.11.1999

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-321749 ✓

(43) 公開日 平成9年(1997)12月12日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/14			H 0 4 L 9/00	6 4 1
G 0 6 F 15/00	3 3 0		G 0 6 F 15/00	3 3 0 A
G 0 9 C 1/00	6 6 0	7259-5 J	G 0 9 C 1/00	6 6 0 E
		7259-5 J		6 6 0 A
H 0 4 L 9/10			H 0 4 L 9/00	6 2 1 Z
審査請求 有 請求項の数 3 O L (全 6 頁)				

(21) 出願番号 特願平8-134823

(22) 出願日 平成8年(1996)5月29日

(71) 出願人 000213301

中部日本電気ソフトウェア株式会社

愛知県日進市米野木町南山500番地20

(72) 発明者 南條 正之

愛知県日進市米野木町南山500番地20 中

部日本電気ソフトウェア株式会社内

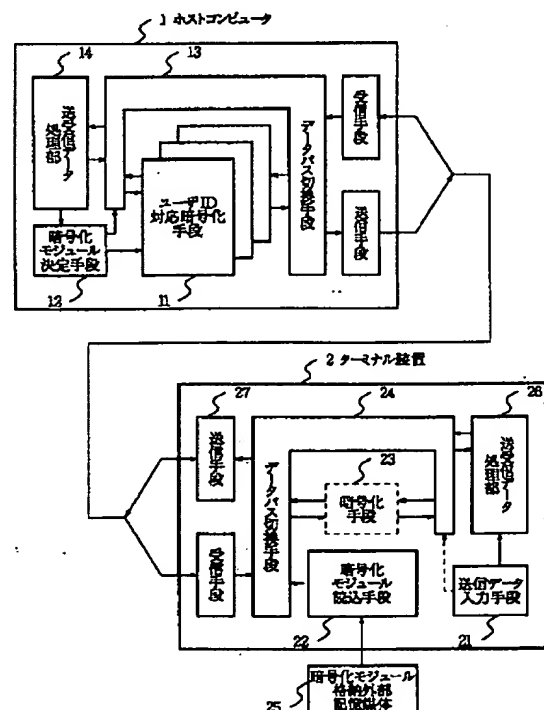
(74) 代理人 弁理士 京本 直樹 (外2名)

(54) 【発明の名称】 オンラインセキュリティ制御方式

(57) 【要約】

【課題】 ログオン後は、ホストコンピュータ、ターミナル装置間で送受信するデータを暗号化することにより、オンラインシステムでのセキュリティを向上できるオンラインセキュリティ制御方式を提供することにある。

【解決手段】 ホストコンピュータ 1 ではユーザ ID およびパスワードの正当性をチェック後ユーザ ID に応じたユーザ ID 対応暗号化手段 11 を選択してユーザ固有の暗号化および復号化を行ない、ターミナル装置 2 では、ユーザ固有の暗号化モジュールを可搬の外部記憶媒体 25 から暗号化手段 23 に読み出してユーザ固有の暗号化および復号化を行ないセキュリティを確保する。



【特許請求の範囲】

【請求項 1】 ターミナル装置側には、送受信データを暗号／復号化する利用者固有の暗号化モジュールを格納する可搬の外部記憶媒体と、前記暗号化モジュールを読み込む暗号化モジュール読込手段と、前記読み込まれた暗号化モジュールにより送信データを暗号化し受信データを復号化する暗号化手段と、送受信データを前記暗号化手段により暗号／復号化する可否かを切り換える第 1 のデータパス切換手段と、ユーザ ID やパスワードを含む送信データを入力する送信データ入力手段とを有し、ホストコンピュータ側には、それぞれユーザ ID に一意に対応して送受信データを暗号／復号化する複数のユーザ ID 対応暗号化手段と、前記ターミナル装置から送信されたユーザ ID に応じてこれに対応する前記ユーザ ID 対応暗号化手段を決定する暗号化決定手段と、通常は前記ユーザ ID 対応暗号化手段を経由しないパスを形成し前記決定に応じて前記ユーザ ID 対応暗号化手段を経由するパスを形成する第 2 のデータパス切換手段とを有することを特徴とするオンラインセキュリティ制御方式。

【請求項 2】 第 1 のデータパス切換手段は暗号化モジュール読み取りに応じて起動することを特徴とする請求項 1 記載のオンラインセキュリティ制御方式。

【請求項 3】 第 1 のデータパス切換手段は送信データ入力手段からの特定の入力に応じて起動することを特徴とする請求項 1 記載のオンラインセキュリティ制御方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はオンラインセキュリティ制御方式に関し、特にログオン後、送受信データをユーザ ID に対応した暗号化モジュールによって暗号化するオンラインセキュリティ制御方式に関する。

【0002】

【従来の技術】従来のオンラインセキュリティ制御方式は、利用者固有のユーザ ID およびパスワードをターミナル装置からホストコンピュータに入力送信し、ホストコンピュータ内で正当性をチェックすることで行なわれていた。

【0003】また、特開平 04-160666 号公報に示される技術では、予めユーザとその使用装置とを登録しておき、ユーザ ID およびパスワードの正当性チェック以外に使用されている装置の正当性をチェックすることで不正な接続を防ぐ方式がとられていた。

【0004】

【発明が解決しようとする課題】上述した従来のオンラインセキュリティ制御方式では、ユーザ ID およびパスワードは、指紋や装置 ID のような人や装置に対して固有なものではなく利用者が記憶しているだけの情報であり、第三者が何らかの手段によってユーザ ID およびパ

スワードを知ることによって不正にオンラインシステムに入り込めることができるという問題点を有している。

【0005】また、特開平 04-160666 号公報に見られるような装置 ID を正当性をチェックする際の情報に加えた場合、運用上使用できるターミナル装置が限定されるため柔軟性がなく、また、新たに装置を追加する場合や撤去する場合には、ターミナル装置の管理が煩雑になるという欠点がある。

【0006】本発明の目的は、ログオン後は、ホストコンピュータ、ターミナル装置間で送受信するデータを暗号化し、また、ターミナル装置側ではメモリカードやフレキシブルディスクのような可搬の外部記憶媒体に格納した暗号化モジュール（プログラム）を使用することにより、オンラインシステムでのセキュリティを向上させ、運用上のターミナル装置の管理を軽減できるオンラインセキュリティ制御方式を提供することにある。

【0007】

【課題を解決するための手段】第 1 の発明のオンラインセキュリティ制御方式は、ターミナル装置側には、送受信データを暗号／復号化する利用者固有の暗号化モジュールを格納する可搬の外部記憶媒体と、前記暗号化モジュールを読み込む暗号化モジュール読込手段と、前記読み込まれた暗号化モジュールにより送信データを暗号化し受信データを復号化する暗号化手段と、送受信データを前記暗号化手段により暗号／復号化する可否かを切り換える第 1 のデータパス切換手段と、ユーザ ID やパスワードを含む送信データを入力する送信データ入力手段とを有し、ホストコンピュータ側には、それぞれユーザ ID に一意に対応して送受信データを暗号／復号化する複数のユーザ ID 対応暗号化手段と、前記ターミナル装置から送信されたユーザ ID に応じてこれに対応する前記ユーザ ID 対応暗号化手段を決定する暗号化決定手段と、通常は前記ユーザ ID 対応暗号化手段を経由しないパスを形成し前記決定に応じて前記ユーザ ID 対応暗号化手段を経由するパスを形成する第 2 のデータパス切換手段とを有して構成される。

【0008】第 2 の発明のオンラインセキュリティ制御方式は、第 1 の発明のオンラインセキュリティ制御方式において、第 1 のデータパス切換手段は暗号化モジュール読み取りに応じて起動することを特徴としている。

【0009】第 3 の発明のオンラインセキュリティ制御方式は、第 1 の発明のオンラインセキュリティ制御方式において、第 1 のデータパス切換手段は送信データ入力手段からの特定の入力に応じて起動することを特徴としている。

【0010】【作用】ターミナル装置から利用者が自分のユーザ ID およびパスワードを送信後、ターミナル装置内の暗号化モジュール読込手段が外部記憶媒体中の利用者に固有の暗号化モジュールをターミナル装置内に組み込む。

3

【0011】一方、ホストコンピュータでは、ターミナル装置から送信されたユーザIDをもとにホストコンピュータ内の暗号化モジュール決定手段がユーザIDに対応する暗号化モジュールの中から使用する暗号化モジュールを決定する。

【0012】これ以降、ホストコンピュータとターミナル装置間で送受信するデータはホストコンピュータ内の暗号化モジュールとターミナル装置内の暗号化モジュールによって暗号化される。

【0013】このため、利用者固有のターミナル装置側の暗号化モジュールを持たない不正な利用者は、意図する不正行為を実行できない。

【0014】また、ターミナル装置が変わっても暗号化モジュールが格納された外部記憶媒体をセットすることによりターミナル装置の管理情報を変更することなく利用できる。

【0015】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

図1は本発明のオンラインセキュリティ制御方式の一実施の形態を示すブロック図である。

【0017】本実施の形態のオンラインセキュリティ制御方式は、図1に示すように、ターミナル装置2内に、送受信データを暗号／復号化する利用者固有の暗号化モジュールを格納する暗号化モジュール格納外部記憶媒体25と、この暗号化モジュール格納外部記憶媒体25から暗号化モジュールを暗号化手段23内のメモリに読み込む暗号化モジュール読込手段22と、ホストコンピュータ1へ送信するユーザIDやパスワードデータを利用者に入力させる送信データ入力手段21と、送受信データを暗号化モジュールにより暗号化する暗号化手段23と、暗号化手段23によって暗号／復号化する可否かを切り換えるデータパス切換手段24とを有している。

【0018】一方、ホストコンピュータ1内には、ユーザIDに一意に対応し送受信データを暗号／復号化するユーザID対応暗号化手段11と、ターミナル装置2から送信されたユーザIDにより対応するユーザID対応暗号化手段11を決定する暗号化モジュール決定手段12と、ユーザID対応暗号化手段11を決定後送信データをユーザID対応暗号化手段11によって暗号／復号化する処理に切り換えるデータパス切換手段13とを有している。

【0019】暗号化モジュール格納外部記憶媒体25はフレキシブルディスクやメモ리카ード等可搬性が高いものが望ましい。

【0020】暗号化モジュール格納外部記憶媒体25に格納されている暗号化モジュールはコード変換テーブルにより送受信データを暗号／復号化するものや計算により暗号／復号化するもの等がある。

【0021】データパス切換手段24は送信データ入力

4

手段21がユーザIDやパスワードデータ送信して後に暗号化モジュールを読み取りその後、自動的に切り換える方式と利用者がキーボード操作により任意の時点で切り換える方式等がある。

【0022】次に、本実施の形態のオンラインセキュリティ制御方式の動作について、図1を参照して詳細に説明する。

【0023】オンライン処理を開始する場合、ターミナル装置2内の送信データ入力手段21を使用して利用者は自分のユーザIDおよびパスワードを入力する。

【0024】入力されたデータは、受信データの画面表示やキーボード入力データ、ファイルデータの送信データ編集等の従来のデータ処理を行なう送受信データ処理部26を経由しデータパス切換手段24に供給される。

【0025】オンライン処理開始時は暗号化を行なわないパスを規定値として暗号化手段23を経由せずそのまま送信手段27からホストコンピュータ1に送信される。

【0026】ターミナル装置2からのユーザIDおよびパスワードデータをホストコンピュータ1が受信すると、ユーザIDおよびパスワードデータはデータパス切換手段13に供給され暗号化を行なわないパスを規定値としてユーザID対応暗号化手段11を経由せずそのまま送受信データ処理部14に供給される。

【0027】送受信データ処理部14でユーザIDおよびパスワードの正当性をチェックし、正しければ暗号化モジュール決定手段12によってユーザIDに対応するユーザID対応暗号化手段11を決定し、データパス切換手段13によって暗号化を行なうパスに切り換える。

【0028】一方、ターミナル装置2において、ユーザIDおよびパスワードが正当とホストコンピュータ1に判断されたことを認知できた時点で暗号化モジュール読込手段22を使用して暗号化モジュール格納外部記憶媒体25の暗号化モジュールを暗号化手段23内に読み込み、その後、データパス切換手段24は暗号化を行なうパスに切り換える。

【0029】これ以降、ホストコンピュータ1とターミナル装置2との間で送受信されるデータは、ホストコンピュータ1内のユーザID対応暗号化手段11によって、また、ターミナル装置2内の暗号化手段23によって暗号／復号化される。

【0030】次に、本発明の実施例について図面を参照して説明する。

【0031】図2を参照すると、本発明の実施例のオンラインセキュリティ制御方式のターミナル装置30はパソコン通信を行なうターミナル装置30であり、モデム40経由で公衆回線に接続する。

【0032】図1と図2とを対比すると、暗号化モジュールを格納する暗号化モジュール格納外部記憶媒体25は暗号化モジュール格納フレキシブルディスク35であ

り、暗号化モジュール読込手段22はフレキシブルディスク装置32であり、送信データ入力手段21はキーボード31としてある。

【0033】暗号化モジュールは、図3(c)に示す受信データ変換テーブル23-Rと図3(d)に示す送信データ変換テーブル23-Sとを持ち、受信データおよび送信データをテーブル引きにて変換する方式である。

【0034】暗号／復号化するか否かの切り換えは利用者のキーボード31からの指示によってデータパス切換手段24が行なう。

【0035】ホストコンピュータ1側はターミナル装置30から正しいパスワードを受信した時点で暗号化モジュールを経由するパスに切り換えるものとする。

【0036】次に、本発明の実施例の動作について、図2、3および4の参照して詳細に説明する。

【0037】図2を参照すると、ターミナル装置30側の暗号化手段23を制御する暗号化モジュールは暗号化モジュール格納フレキシブルディスク35に格納されており、降順のアルファベットのそれぞれの文字を昇順のアルファベットのそれぞれの文字に順に対応して変換する受信データ変換テーブル23-Rと送信データ変換テーブル23-Sとを持ち、図3(a)および(b)の流れ図に示すように、送受信データをこれらのテーブル引きにより変換する暗号化方式をとる。

【0038】パソコン通信を開始すると、受信データを画面に表示したりキーボード31からの入力データを送信する従来の通信処理を行なう送受信データ処理部26がキーボード入力送信データや受信データ表示を行なう。このとき、ターミナル装置30内のデータパスは暗号化を行なわないパスとなっており送受信データは暗号化手段23を経由することはない。

【0039】まず、暗号化しない通常の場合について説明する。

【0040】パソコン通信では通常図4(a)に示すように、ユーザIDおよびパスワードをターミナル装置30からモデム40経由でホストコンピュータ1に送信し(図4(a)a-1)、ホストコンピュータ1側で正当性をチェックし正しければ処理を続行できる仕組みとなっている。

【0041】よって、利用者にとってはユーザIDおよびパスワード入力後次に続くべきメッセージを受信することで(図4(a)a-2)、ユーザIDおよびパスワードがホストコンピュータ1側で確認されたことを判断でき、以後、継続して通信を行なうことができる。これが従来の方式である。

【0042】次にまず、ホストコンピュータ1が暗号化対応した場合についての動作を説明する。

【0043】パスワード入力送信後(図4(b)b-1)、ホストコンピュータ1は次に続くべきメッセージを暗号化してターミナル装置30に送信し(図4(b)

b-2)、ターミナル装置30からの入力送信待ちとなる。

【0044】暗号化モジュールを持たない不正な利用者が接続を試みた場合は、受信したデータは暗号化されたデータである図4(b)b-2の「プロファイルシェウセイシマスカ(B, M, TD)=」までのデータ表示となっており、対応する暗号化モジュール格納フレキシブルディスク35を持っていないので、復号化することができず、その後の意図する不正行為を行なうことができない。

【0045】しかし、正常利用者の場合には、暗号化モジュール格納フレキシブルディスク35をフレキシブルディスク装置32にセットしキーボード31の操作によりデータパス切換手段24にデータパス切り換えを要求する。

【0046】データパス切換手段24はフレキシブルディスク装置32にセットされた暗号化モジュール格納フレキシブルディスク35内の暗号化モジュールを暗号化手段23内に読み込み、ターミナル装置30のデータパスを暗号化を行なうパスに切り換え暗号化対応を行なう。

【0047】このデータパス切り換えによってターミナル装置30はホストコンピュータ1から送られてくる暗号化された受信データを暗号化手段23によって復号化し、送受信データ処理部26で、例えばキーボード31よりの2度の「N」入力を経て、図4(b)b-2の「お知らせを表示しますか(Y, N)=N」までのように表示し、正常利用者は相続いて次のキーボード入力送信を暗号化手段23によって暗号化して送信することとなる。

【0048】以上説明したように、本実施の形態および実施例のオンラインセキュリティ制御方式は、ログオン後、ホストコンピュータとターミナル装置の間で送受信するデータをユーザIDに対応した方式で暗号化するため、暗号化モジュールを持たない不正な利用者が意図する不正行為を行なうことができず、これにより機密情報の入手やデータの改竄、破壊等の不正な利用者の悪意による行為を防ぐことができる。

【0049】また、可搬性のある外部記憶媒体に利用者固有の暗号化モジュールを格納するので、装置IDを使用している特開平04-160666号公報記載の技術のように利用できるターミナル装置に限定されず任意のターミナル装置でオンライン処理を行なうことができ、これによりターミナル装置を追加または撤去する場合、ターミナル装置の管理情報等を変更する必要はなく、管理の簡単化ができる。

【0050】

【発明の効果】以上説明したように、本発明のオンラインセキュリティ制御方式は、ログオン後、ホストコンピュータとターミナル装置の間で送受信するデータをユー

10

20

30

40

50

7

ザIDに対応した方式で暗号化するため、暗号化モジュールを持たない不正な利用者が意図する不正行為を行なうことができず、これにより機密情報の入手やデータの改竄、破壊等の不正な利用者の悪意による行為を防ぐことができるという効果を有する。

【0051】また、可搬性のある外部記憶媒体に利用者固有の暗号化モジュールを格納するので、装置IDを使用している特開平04-160666号公報記載の技術のように利用できるターミナル装置に限定されず任意のターミナル装置でオンライン処理を行なうことができ、これによりターミナル装置を追加または撤去する場合、ターミナル装置の管理情報等を変更する必要はなく、管理の簡単化ができるという効果を有している。

【図面の簡単な説明】

【図1】本発明のオンラインセキュリティ制御方式の一実施の形態を示すブロック図である。

【図2】本発明のオンラインセキュリティ制御方式の一実施例のターミナル装置の構成を示すブロック図である。

【図3】(a)は本発明のオンラインセキュリティ制御方式の一実施例のデータ受信時の動作を示す流れ図、

(b)はデータ送信時の動作を示す流れ図、(c)は受

8

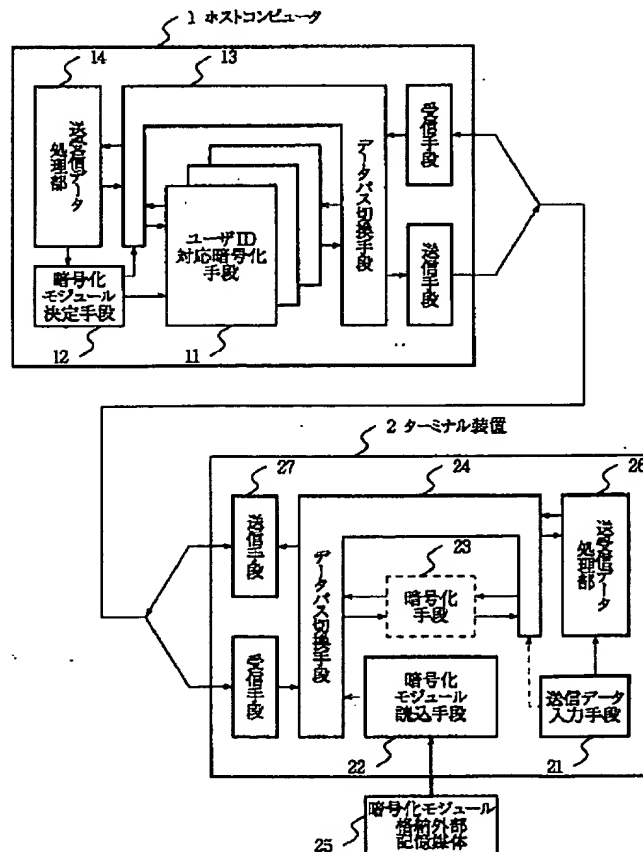
信データ変換テーブルを示すテーブル図、(d)は送信データ変換テーブルを示すテーブル図である。

【図4】(a)は従来の暗号化しないときのターミナル装置に表示されるメッセージ表示図、(b)は暗号化対応した場合のターミナル装置に表示されるメッセージ表示図である。

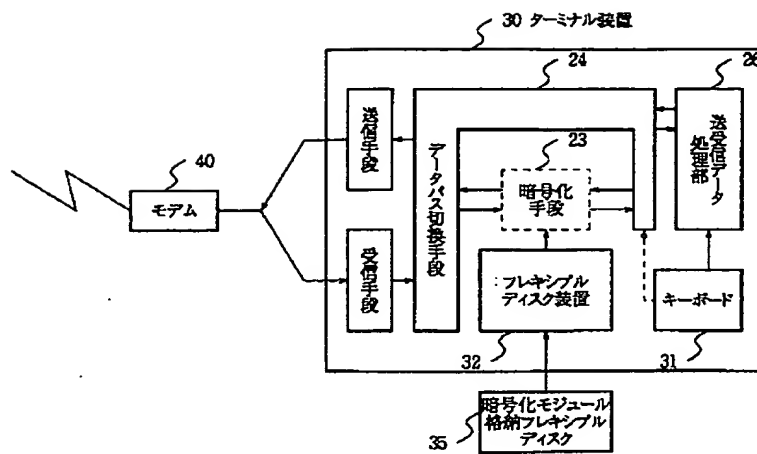
【符号の説明】

- | | |
|-------|----------------------|
| 1 | ホストコンピュータ |
| 2、30 | ターミナル装置 |
| 11 | ユーザID対応暗号化手段 |
| 12 | 暗号化モジュール決定手段 |
| 13、24 | データバス切替手段 |
| 14、26 | 送受信データ処理部 |
| 21 | 送信データ入力手段 |
| 22 | 暗号化モジュール読込手段 |
| 23 | 暗号化手段 |
| 25 | 暗号化モジュール格納外部記憶媒体 |
| 27 | 送信手段 |
| 31 | キーボード |
| 32 | フレキシブルディスク装置 |
| 35 | 暗号化モジュール格納フレキシブルディスク |
| 40 | モデム |

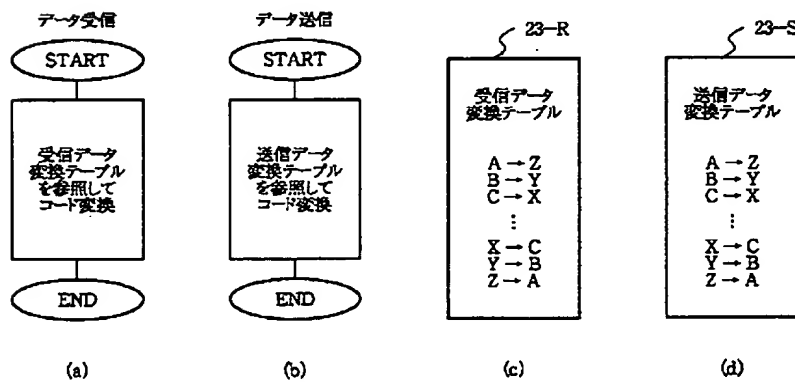
【図1】



【図2】



【図3】



【図4】

